

WHAT IS CLAIMED IS:

1. A method for securing a data object, comprising:
providing a data object comprising digital data and file format information;
embedding independent data into the data object; and
5 scrambling the data object to degrade the data object to a predetermined
signal quality level.
2. The method of claim 1, further comprising the step of performing the
steps of embedding and scrambling until a predetermined condition is met.
- 10 3. The method of claim 2, wherein the predetermined condition
comprises reaching a desired signal quality level of the data object.
4. The method of claim 1, further comprising the steps of:
15 descrambling the data object to upgrade the data object to a predetermined
signal quality level; and
decoding the embedded independent data.
5. The method of claim 4, further comprising the step of performing the
20 steps of embedding and scrambling until a predetermined condition is met.
6. The method of claim 5, wherein the predetermined condition
comprises reaching a desired signal quality level of the data object.
- 25 7. The method of claim 1, wherein the predetermined signal quality
level is selected from the group consisting of telephone quality, radio quality, MP3
quality, and CD quality.
8. The method of claim 1, wherein the predetermined signal quality
30 level is selected from the group consisting of NTSC quality, QuickTime quality,
Macrovision quality, satellite quality, high definition quality, and DVD quality.

9. The method of claim 1, wherein the independent data comprises authenticatable data.

10. The method of claim 9, wherein the authenticatable data comprises a robust open watermark.

11. The method of claim 4, wherein the step of decoding the embedded independent data comprises using a public key is used to decode the independent data.

10

12. The method of claim 1, wherein the data object comprises at least one of digital music, video, and at least one image.

13. The method of claim 1, further comprising the step of:
15 scrambling the independent data before the embedding step so that the embedding step embeds the scrambled independent data into the data object.

14. A method for distributing a data signal, comprising:
providing a data signal comprising digital data and file format information;
20 selecting a first scrambling technique to apply to the data signal;
scrambling the data signal using the first scrambling technique, resulting in a first-level degraded data signal;

creating a first descrambling key for the first-level degraded data signal based on the first scrambling technique;
25 selecting a second scrambling technique to apply to the first-level degraded data signal;

scrambling the first-level degraded data signal using a second scrambling technique, resulting in a second-level degraded data signal; and
creating a second descrambling key for the second-level degraded data signal
30 based on the second scrambling technique.

15. The method of claim 14, further comprising:

associating a first payment level with the data signal;
associating a second payment level with the first-level degraded data signal;
and
associating a third payment level with the second-level degraded data signal.

5

16. The method of claim 15, further comprising:
selecting a payment level; and
applying at least one of the descrambling keys to the second-level degraded
data signal, resulting the associated data signal.

10

17. The method of claim 14, wherein at least one of the first scrambling
technique and the second scrambling technique comprises manipulation of the file
format information.

15

18. The method of claim 14, wherein at least one of the first scrambling
technique and the second scrambling technique comprises a cryptographic cipher.

19.

The method of claim 14, wherein the signal quality levels are selected
from the group consisting of CD quality, MP3 quality, radio quality, and telephone
quality.

20

20.

The method of claim 14, wherein the predetermined signal quality
level is selected from the group consisting of NTSC quality, QuickTime quality,
Macrovision quality, satellite quality, and DVD quality.

25

21.

A method for distributing a data object, comprising:
providing a data object comprising digital data and file format information;
encoding independent authentication data into the data object; and
manipulating the file format information based on at least one signal
characteristic of the data object.

30

22. The method of claim 21, wherein the independent authentication data is steganographically encoded into the data object.

23. The method of claim 21, wherein the independent authentication data
5 comprises a robust open watermark.

24. The method of claim 21, wherein the at least one signal characteristic of the data object comprises file format information.

10 25. The method of claim 21, further comprising the step of:
generating at least one cryptographic key based on a result of the manipulation of the file format information.

26. The method of claim 25, wherein the step of generating at least one
15 cryptographic key based on a result of the manipulation of the file format information comprises:

selecting at least one of a plurality of signal characteristics of the data format; and

20 ciphering the results of the order of steps of signal characteristic selection.

27. The method of claim 21, wherein the step of manipulating the file format information based on at least one signal characteristic of the data object comprises multiple step manipulation, and an order of the multiple step manipulation is ciphered to generate a predetermined key.

25 28. The method of claim 21, wherein the steps of encoding independent authentication data into the data object and manipulating the file format information based on at least one signal characteristic of the data object comprise multiple step encoding and manipulation, and an order of the multiple steps is ciphered to
30 generate a predetermined key.

29. The method of claim 21, further comprising:

generating at least one cryptographic key having a logical relationship with the manipulation of the file format information and the steganographic encoding method.

- 5 30. The method of claim 21, further comprising:
generating an authorization key that is dependent on the a public key and a private key;
wherein the authorization key is further dependent on at least one of a time, a channel, and an object.

10

31. A method for distributing data signals, comprising:
embedding independent data into a data object;
scrambling the data object;
distributing the scrambled data object;
15 distributing at least one predetermined key that enables access to the data object; and
descrambling the scrambled data object with the predetermined key.

- 20 32. The method of claim 31, wherein the independent data comprises payment information.

33. The method of claim 31, wherein the independent data comprises authentication information.

- 25 34. The method of claim 31, wherein the independent data comprises a one-way hash.

35. The method of claim 31, wherein the independent data comprises a digital signature.

30

36. The method of claim 31, wherein the independent data comprises a time stamp.

37. The method of claim 31, wherein the steps of embedding independent data into a data object and scrambling the data object each has a logical relationship with the generation of the predetermined key.

5

38. The method of claim 31, wherein the steps of embedding independent data into a data object and scrambling the data object each has a logical relationship with the generation of the predetermined key and a communications channel for which the data signal is being prepared.

10

39. The method of claim 31, wherein the step of descrambling the scrambled data object comprises:

initiating the transmission of a recipient public key from an intended recipient of the data object to a sender of the data object; and

15

initiating the transmission of a sender session key from the sender to the recipient to initiate descrambling of the embedded independent data.

40. The method of claim 31, wherein the step of descrambling the scrambled data object comprises:

20

initiating a session key-based exchange between a sender and receiver;
wherein the session key is dependent on at least one of a channel, a time, and a data object.

41. The method of claim 31, wherein the step of descrambling the scrambled data object comprises:

25

initiating a session key-based exchange between a sender and a receiver that is a timing based timing mechanism.

42. The method of claim 31, wherein the step of descrambling the scrambled data object comprises:

30

initiating a pooling of similar session keys.

43. The method of claim 31, wherein the step of descrambling the scrambled data object comprises:

logically associating a signal quality with a predetermined estimation of a bandwidth requirement for the session.

5

44. The method of claim 31, wherein the step of descrambling the scrambled data object comprises:

logically associating a signal quality with a bandwidth allocation model.

10

45. The method of claim 31, wherein the step of descrambling the scrambled data object comprises:

logically associating a signal quality with a signal quality parameter.

15

46. The method of claim 31, wherein the step of descrambling the scrambled data object comprises:

updating a signal quality of the data object based on an approval of the session keys by the originating data signal server.

20

47. The method of claim 31, wherein the step of scrambling the data object comprises:

manipulating file format information of the data object.

48. The method of claim 31, wherein the step of scrambling the data object comprises:

25

scrambling the data object with a cryptographic cipher.

49. A method for data signal distribution comprising:

applying a steganographic technique for embedding independent data into the data signal;

30

applying a scrambling technique selected from the group consisting of file format manipulation and partial encryption; and

generating a predetermined key.

50. The method of claim 49, wherein the file format manipulation scrambling technique has a relationship with at least one signal characteristic of the data signal.

5

51. The method of claim 49, wherein the partial encryption scrambling technique is unrelated to any characteristic of the data signal.

52. The method of claim 49, wherein the partial encryption scrambling technique degrades a signal quality of the data signal.

10

53. The method of claim 49, wherein the predetermined key enables descrambling of the signal.

54. The method of claim 49, wherein the predetermined key is based on unique identifying information for a receiver.

15

55. The method of claim 49, wherein the predetermined key is based on a signal quality threshold that is adjustable in at least one of a time, a frequency, and a bit depth.

20

56. The method of claim 49, wherein the predetermined key is based on a signal quality threshold that is adjustable in at least one of a time, a frequency, a bit depth, and a measure of payment that may be adjusted for at least one of a time, a frequency, and a bit depth.

25

57. The method of claim 49, wherein the predetermined key is pregenerated based on at least one expected characteristic of the data signal.

58. The method of claim 49, wherein the predetermined key is divisible into a plurality of discrete partial keys, each discrete partial key representing less than an entire payment for the data signal.

30

59. The method of claim 49, wherein the predetermined key can be broken into a plurality of discrete partial keys, each discrete partial key representing less than an entire descrambled state for the data signal.

5

60. A method for bandwidth allocation, comprising:
presenting a plurality of data objects to a user, each data object having a security application;
linking at least a first data object to at least one second data object;
10 wherein a characteristic of the first data object causes a change in the second data object.

61. The method of claim 60, wherein the first data object comprises advertising.

15

62. The method of claim 60, wherein an increased quantity of the first data object causes a signal quality level of the second data object to increase.

63. The method of claim 60, wherein a signal quality level of the second
20 data object is increased with a predetermined key.

64. The method of claim 63, wherein the predetermined key comprises at least one session key.

25 65. The method of claim 64, wherein the at least one session key adjusts a payment for the second data object.

66. A system for securing data within a data object, comprising:
an embedder that embeds independent data into a data object; and
30 a scrambler that scrambles the data object to degrade the data object to a predetermined signal quality level.

a descrambler that descrambles the data object to upgrade the data object to a predetermined signal quality level; and

a decoder that decodes the embedded independent data.

68. A system for distributing a data signal, comprising:

10 a first scrambler that scrambles the data signal using the first scrambling technique, resulting in a first-level degraded data signal;

a second selector that selects a second scrambling technique to apply to the first-level degraded data signal;

a second key creator that creates a second descrambling key for the second-level degraded data signal based on the second scrambling technique.